JOURNAL OF ALGEBRA 79, 307–318 (1982)

Simple Quandles

DAVID JOYCE

Department of Mathematics, Clark University, Worcester, Massachusetts 01610

Communicated by Saunders MacLane

Received November 4, 1981

Quandles have two operations corresponding to the operations of conjugation $x \rhd y = y^{-1}xy$ and $x \rhd^{-1} y = yxy^{-1}$ in a group. Simple quandles are classified in terms of certain triples $\langle N, C, m\rangle$, where N is a simple group, C is a conjugacy class in Aut N, and $m \geqslant 1$.

The concept of "quandle," introduced in [5], captures the equational content of the two operations of conjugation $x \rhd y = y^{-1}xy$ and $x \rhd^{-1} y = yxy^{-1}$ in a group. Two theories are needed in order to study the structure of an algebra such as a quandle. A general decomposition theory involving a form of the Jordan–Hölder–Schreier theorem has been eveloped by Goldie [3] and by Grätzer [4, pp. 74–75]. This general theory does to some degree specialize to quandles. There remains the need for a classification of the simple algebras. In this article simple quandles are classified by associating to each one a simple group, a conjugacy class of automorphisms of that group, and a positive integer. In the discussion that follows the term "simple group" is meant to include prime cyclic groups. When prime cyclic groups are to be excluded then the term "nonabelian simple group" will be used. This article is self-contained; no knowledge of [5] is required.

1. PRELIMINARY CONCEPTS

A *quandle* is a set equipped with two binary operations denoted $x \rhd y$ and $x \rhd^{-1} y$ satisfying three identities:

Q1. $x \rhd x = x$.

Q2. $(x \rhd y) \rhd^{-1} y = x = (x \rhd^{-1} y) \rhd y$.

Q3. $(x \rhd y) \rhd z = (x \rhd z) \rhd (y \rhd z)$.

0021-8693/82/120307-12$02.00/0

Whenever we speak of a group or of a conjugacy class in a group as a quandle, we mean with the two operations

$$x \rhd y = y^{-1}xy \qquad \text{and} \qquad x \rhd^{-1} y = yxy^{-1}.$$

A quandle is said to be *abelian* if it satisfies the identity

QAb. $(w \rhd x) \rhd (y \rhd z) = (w \rhd y) \rhd (x \rhd z)$.

Axiom Q2 assures us that to each element y of a quandle Q there is a bijection on Q whose value at x is $x \rhd y$. We call this bijection the *symmetry at* y denoted $S(y)$. Axiom Q3 asserts that the symmetry at z preserves one quandle operation. It follows that each symmetry is actually a quandle automorphism of Q. The group of automorphisms of Q generated by the symmetries of its elements is called the *inner automorphism group* of Q, denoted Inn Q. It is convenient to have Inn Q act on the right on Q (evaluate the automorphism a at the element x giving $x \cdot a$) and to write the composition of two automophisms a and b as ab rather than $b \circ a$. The function $S\colon Q \to \text{Inn } Q$ is a quandle homomorphism when Inn Q is treated as a quandle, that is, $S(x \rhd y) = S(y)^{-1} S(x) S(y)$. More generally, for x in Q and a in Inn Q, we have $S(x \cdot a) = a^{-1}S(x)a$.

A quandle Q is said to be *algebraically connected* if Inn Q acts transitively on Q, that is, given two elements x and z in Q there exists a sequence of elements $y_1, y_2, \ldots, y_n$ in Q and a sequence of exponents $e_1, e_2, \ldots, e_n$ in $\{1, -1\}$ such that

$$x \cdot S(y_1)^{e_1} S(y_2)^{e_2} \cdots S(y_n)^{e_n} = z.$$

Any quandle has a quotient (i.e., homomorphic image) whose elements are its algebraically connected components and whose operations are first projections (i.e., $x \rhd y = x \rhd^{-1} y = x$).

The *transvection group*, Trans Q, of a quandle Q is defined to be the subgroup of Inn Q generated by the elements of the form $S(x) S(y)^{-1}$ for x and y in Q. The quotient group Inn Q/Trans Q is a cyclic group since any two generators $S(x)$ and $S(y)$ of Inn Q are congruent modulo Trans Q. The order of this quotient group, which is the index of Trans Q in Inn Q, is called the *transvection index* of Q, which may be finite or infinite. The commutator subgroup $(\text{Inn } Q)'$ of Inn Q is always contained in Trans Q. If Q is algebraically connected, then $(\text{Inn } Q)'$ equals Trans Q. Indeed, in that case each generator $S(x) S(y)^{-1}$ of Trans Q is of the form $S(x) a^{-1} S(x)^{-1} a$, since there is an a in Inn Q such that $y = x \cdot a$ and so $S(y) = S(x \cdot a) = a^{-1}S(x)a$.

Remark. A quandle is abelian iff its transvection group is abelian.

Proof. By definition a quandle Q is abelian iff the identity QAb holds in

Q. Equivalently, for all x, y, and z in Q it is the case that $S(x)\,S(z)^{-1}\,S(y) = S(y)\,S(z)^{-1}\,S(x)$. On the other hand, Trans Q is abelian iff the following identity holds:

$$S(x)\,S(z)^{-1}\,S(y)\,S(t)^{-1} = S(y)\,S(t)^{-1}\,S(x)\,S(z)^{-1}.$$

By setting $t = z$ we find that if Trans Q is abelian, then Q is abelian. Conversely, if Q is abelian, then we have

$$\begin{aligned} S(x)\,S(z)^{-1}\,S(y)\,S(t)^{-1} &= S(y)\,S(z)^{-1}\,S(x)\,S(t)^{-1} \\ &= S(y)\,S(t)^{-1}\,S(x)\,S(z)^{-1}, \end{aligned}$$

which implies that Trans Q is abelian. ∎

2. Simple Quandles

We say that a quandle is *simple* if it has no quotients except itself and the one-element quandle. An equivalent condition is that every homomorphism from the quandle is either constant or a monomorphism.

We will uncover the relations between simple quandles and groups in a series of lemmas. Although not every quandle imbeds in a group, we first show that simple quandles imbed in groups, moreover, that a simple quandle appears as a generating conjugacy class in some group, namely, its inner automorphism group. After characterizing inner automorphism groups of simple quandles, we study the structure of these groups in the case when the quandle has finite transvection index. The lemmas culminate in a theorem which states a correspondence between simple quandles of finite transvection index and certain triples $\langle N, C, m\rangle$, where N is a simple group, C is a conjugacy class in Aut N, and $m \leqslant 1$.

Lemma 1. *Let Q be a simple quandle whose order is greater than two. Let $G = \operatorname{Inn} Q$. Then*

(i) *$S: Q \to G$ is an injection.*

(ii) *Q is algebraically connected.*

(iii) *$S(Q)$ is a generating conjugacy class in G.*

(iv) Trans $Q = G'$.

(v) *G/G' is cyclic.*

(vi) *The center of G, $Z(G)$, is trivial.*

Proof. (i) If S is not an injection, then it identities all elements in which case the identity $x \rhd y = x$ holds in Q. But the only simple quandles satisfying $x \rhd y = x$ have no more than two elements.

(ii) Just consider the quotient of Q whose elements are its algebraic components.

(iii) The image of Q, $S(Q)$, always generates G. It is a conjugacy class since Q is algebraically connected. Parts (iv) and (v) also follow from algebraic connectivity as mentioned in Section 1.

(vi) Let a lie in the center of Inn Q. Then for x in Q, we have $S(x) = a^{-1}S(x)a = S(x \cdot a)$. From the injectivity of S it follows that $x = x \cdot a$. Thus, a is the identity automorphism on Q. ∎

Another property of Inn Q that follows from the simplicity of Q is that $(\text{Inn } Q)'$ is the smallest nontrivial normal subgroup of Inn Q. Since we will need a converse to this statement, this fact is best stated as in the next lemma.

LEMMA 2. *Let G be a group with trivial center, and let Q be a generating conjugacy class of G treated as a quandle. Then $G \cong \text{Inn } Q$ and $G' \cong \text{Trans } Q$. The following three statements are equivalent.*

(i) *Q is a simple quandle.*

(ii) *G' is the smallest nontrivial normal subgroup of G.*

(iii) *G' is a minimal nontrivial normal subgroup of G.*

Proof. For each y in G let $S(y)$ be conjugation by y regarded as an automorphism of Q: for x in Q let $x \cdot S(y)$ be $y^{-1}xy$. Then S is a group homomorphism from G to Inn Q. It is surjective since G includes Q. Assume that y lies in the kernel of S. Then y commutes with all elements of Q. But Q generates G, so y lies in the cneter of G; hence $y = 1$. Thus, the kernel of S is trivial. Therefore, S is a group isomorphism from G onto Inn Q. Since Q is a generating conjugacy class, it is an algebraically connected quandle. Thus $\text{Trans } Q = (\text{Inn } Q)' = S(G')$, i.e., S restricts to an isomorphism from G' onto Trans Q.

(i) $\Rightarrow$ (ii): Let N be a normal subgroup of Inn Q. Define an equivalence relation on Q by

$$x \equiv y \text{ iff there is an } n \text{ in } N \text{ such that } x \cdot n = y.$$

From the normality of N it follows that $\equiv$ is a congruence on Q. When Q is simple, we have only two cases. If $\equiv$ is equality, then N acts trivially on Q, therefore, N consists of the identity alone. If $\equiv$ relates any two elements of Q, then $\text{Trans } Q \subseteq N$. Indeed, given x and y in Q, there is an n in N such that $x \cdot n = y$. An application of S yields $n^{-1}S(x)n = S(y)$, from which it follows that $S(y)\,S(x)^{-1}$ lies in N. Hence, the generators of Trans Q, and, therefore, all of Trans Q lie in N. Thus, (ii) follows from (i).

(iii) $\Rightarrow$ (i): Let $\equiv$ be a congruence on Q. Define a subgroup N of Trans Q by

$$N = \{n \in \text{Trans } Q \mid x \cdot n \equiv x \text{ for all } x \text{ in } Q\}.$$

Then N is a normal subgroup of Inn Q contained in Trans Q. When (iii) holds, then either $N = 1$ or $N = \text{Trans } Q$. If $N = 1$, then $\equiv$ is equality, for if $y \equiv z$, but $y \neq z$, then $1 \neq S(yz^{-1}) \in N$. In the other case, if $N = \text{Trans } Q$, then $\equiv$ relates any two elements of Q. Therefore, (i) follows from (iii). ∎

We can now characterize inner automorphism groups of simple quandles.

PROPOSITION 3. *A nontrivial group G is isomorphic to the inner automorphism group of a simple quandle iff the following three conditions are satisfied.*

(i) *The center of G, $Z(G)$, is trivial.*

(ii) *G/G' is cyclic.*

(iii) *G' is the smallest nontrivial normal subgroup of G.*

Proof. Lemmas 1 and 2 imply that inner automorphism groups of simple quandles have these properties. Assume G satisfies the conditions. Choose any nontrivial element q in G such that q modulo G' generates the cyclic group G/G'. Let Q be the conjugacy class of q in G. It follows from (iii) that the subgroup of G generated by Q is G itself. The rest follows from Lemma 2. ∎

Note that every generating conjugacy class in such a group is a simple quandle. Some of these classes may be isomorphic as quandles. For instance, the alternating group of five letters, A_5, has four nontrivial conjugacy classes two of which are isomorphic as quandles.

3. Simple Quandles with Finite Transvection Index

The structure of Inn Q can be completely determined when Inn Q/Trans Q is finite. This is a rather broad case that includes all finite simple quandles. It also includes all simple k-quandles. A *k-quandle* is a quandle in which the kth power of every symmetry is the identity. The simple 2-quandles are discussed as a case of special interest in Section 4. This broad case also includes some simple quandles which are not k-quandles for any k.

LEMMA 4. *Let G be a group having a minimal nontrivial normal subgroup T. Assume G/T is a finite cyclic group of order n. Let σ be conjugation by an element of G which represents a generator of G/G'. Then*

(i) *For each nontrivial normal subgroup M of T there is a subgroup K of M normal in T and an integer m dividing n such that $\sigma^m K = K$ and T is the internal direct product*

$$T = K \times \sigma K \times \cdots \times \sigma^{m-1} K.$$

(ii) *There is a normal subgroup N of T and an integer m dividing n such that $\sigma^m N = N$, N is a simple group, and*

$$T = N \times \sigma N \times \cdots \times \sigma^{m-1} N.$$

Let N and m be as in (ii). *Let $d = n/m$, and let τ be the automorphism σ^m restricted to N. Then*

(iii) *$Z(G) = 1$ iff τ has order d modulo* Inn N; *that is, d is the smallest positive integer such that τ^d is an inner automorphism of N.*

Proof. Let M be a nontrivial normal subgroup of T. We prove by induction on k that for $k = 0, 1, \ldots, n$ at least one of the following two statements is true.

(a_k) There is a nontrivial subgroup K of M normal in T and an $m \leqslant k$ such that $\sigma^m K = K$ and the first m σ-conjugates of K, namely, K, $\sigma K, \ldots, \sigma^{m-1} K$, have pairwise trivial intersection.

(b_k) There is a nontrivial subgroup K_k of M normal in T such that the first $k+1$ σ-conjugates of K_k, namely, K_k, $\sigma K_k, \ldots, \sigma^k K_k$, have pairwise trivial intersection.

For $k = 0$ let $K_0 = M$ so that (b_0) holds. If (a_{k-1}) holds, then clearly (a_k) also holds. Assume (b_{k-1}) holds. Consider

$$K_k^* = K_{k-1} \cap \sigma^k K_{k-1} \cap \cdots \cap \sigma^{k(n-1)} K_{k-1}.$$

In case $K_k^* \neq 1$, let $K = K_k^*$ so that (a_k) holds with $m = k$. Otherwise $K_k^* = 1$, in which case let l be least such that

$$1 = K_{k-1} \cap \sigma^k K_{k-1} \cap \cdots \cap \sigma^{kl} K_{k-1}$$

and take

$$K_k = K_{k-1} \cap \sigma^k K_{k-1} \cap \cdots \cap \sigma^{k(l-1)} K_{k-1},$$

which satisfies (b_k).

Since (b_n) cannot hold, we conclude (a_n). Take K and m as in (a_n). Then the internal direct product $K \times \sigma K \times \cdots \times \sigma^{m-1} K$ is a nontrivial normal subgroup of G contained in T, and hence, equals T. Evidently, m divides n. Thus, statement (i) holds.

Choose m to be the largest divisor of n for which there is a normal subgroup N of T such that $\sigma^m N = N$ and $T = N \times \sigma N \times \cdots \times \sigma^{m-1} N$. In order to prove (ii) we only need to show that the only nontrivial normal subgroup of N is N itself. Assume M is a nontrivial normal subgroup of N. Then M is normal in T. An application of (i) supplies us with a subgroup K of M normal in T and a divisor m' of n such that $\sigma^{m'} K = K$ and $T = K \times \sigma K \times \cdots \times \sigma^{m'-1} K$. We conclude from the maximality of m that $m' = m$ and $K = N$. Hence, $M = N$. Thus, statement (ii) holds.

Now σ is conjugation by some element of G representing a generator of G/T; call that element s. Using the fact that each element of G is of the form zs^c, where $z \in T$ and $0 \leqslant c < m$, one sees that the condition $Z(G) = 1$ may be stated in terms of σ as

$$\forall z \in T, \forall c, 0 \leqslant c < n, \text{ if } \sigma(z) = z \text{ and } \sigma^c \text{ is } S(z), \text{ conjugation by } z, \text{ then } z = 1 \text{ and } c = 0.$$

Next, since each element of T is of the form $x_0 \sigma(x_1) \cdots \sigma^{m-1}(x_{m-1})$ where $x_0, x_1, \ldots, x_{m-1} \in N$, we may restate the condition in terms of τ as

$$\forall x \in N, \forall b, 0 \leqslant b < d, \text{ if } \tau(x) = x \text{ and } \tau^b = S(x), \text{ then } x = 1 \text{ and } b = 0. \qquad (*)$$

Clearly, if τ has order d modulo Inn N, then $(*)$ holds, whence, $Z(G) = 1$. Conversely, assume $Z(G) = 1$. Let b be the order of τ modulo Inn N. Clearly, b divides d. Suppose $b \neq d$, so that $0 < b < d$. If N is prime cyclic, then with x the identity element $(*)$ yields $b = 0$, a contradiction. If N is nonabelian simple, then $\tau^b = S(x)$, conjugation by x, for a unique x in N. In that case $\tau^b = S(\tau(x))$ also, so $x = \tau(x)$, and again $(*)$ yields $b = 0$, a contradiction. Thus, the order of τ modulo Inn N is d. ∎

Combining Lemmas 1, 2, and 4 we can associate to a simple quandle Q of finite transvection index a triple $\langle N, \tau, m \rangle$. But before stating this conclusion (Lemma 5), we need a construction of the group G found in Lemma 4 in terms of N, τ, and m.

Let N be a simple group, τ an automorphism of N of order d modulo Inn N, and $m > 0$. Set $n = md$. If N is nonabelian, take z_0 to be the unique element of N such that $\tau^d = S(z_0)$, conjugation by z_0. If N is prime cyclic, let z_0 be the identity element. Using the vector notation $\mathbf{x} = \langle x_0, \ldots, x_{m-1} \rangle$ for elements of N^m, define an automorphism σ of N^m by $\sigma\langle x_0, \ldots, x_{m-1} \rangle = \langle \tau(x_{m-1}), x_0, \ldots, x_{m-2} \rangle$. Let the semidirect product $N^m \ltimes \mathbb{Z}_n$ have the multiplication

$$\langle \mathbf{x}; k \rangle \langle \mathbf{y}; l \rangle = \langle \mathbf{x}\sigma^{-k}(\mathbf{y}); k + l \rangle,$$

where $\mathbf{x}, \mathbf{y} \in N^m$ and $k, l \in \mathbb{Z}_n$. Then $\langle \mathbf{z}; -n \rangle$ lies in the center of $N^m \ltimes \mathbb{Z}_n$,

where $\mathbf{z} = \langle z_0, z_0, \ldots, z_0 \rangle$. Let $G\langle N, \tau, m \rangle$ be the quotient of $N^m \ltimes \mathbb{Z}_n$ modulo the cyclic group generated by $\langle \mathbf{z}; -n \rangle$. Define the quandle $Q\langle N, \tau, m \rangle$ as the conjugacy class of $\langle \mathbf{1}; 1 \rangle$ in $G\langle N, \tau, m \rangle$, where $\mathbf{1} = \langle 1, \ldots, 1 \rangle$. Note that $Q\langle N, \tau, m \rangle = \{ \langle \mathbf{x}; 1 \rangle \in G\langle N, \tau, m \rangle \mid x_0 x_1 \cdots x_{m-1} \in K \}$, where K is the set $K = \{ y^{-1}\tau(y) \in N \mid y \in N \}$. One might simplify the notation for elements of $Q\langle N, \tau, m \rangle$ by noting that $Q\langle N, \tau, m \rangle$ is isomorphic to $\{ \mathbf{x} \in N^m \mid x_0 x_1 \cdots x_{m-1} \in K \}$ along with the operation

$$\mathbf{x} \rhd \mathbf{y} = \sigma(\mathbf{y}^{-1}\mathbf{x})\mathbf{y} = \langle \tau(y_{m-1}^{-1} x_{m-1}) y_0, y_0^{-1} x_0 y_1, \ldots, y_{m-2}^{-1} x_{m-2} y_{m-1} \rangle.$$

In the next lemmas and in the main theorem we complete the correspondence between simple quandles and triples $\langle N, \tau, m \rangle$. We find that two triples determine the same quandle iff their τ's are conjugate in Aut N. This allows us to change the notation to $\langle N, C, m \rangle$, where C is a conjugacy class in Aut N. Finally, we determine which triples $\langle N, C, m \rangle$ yield simple quandles $Q\langle N, C, m \rangle$.

LEMMA 5. *Let Q be a simple quandle of order greater than two having finite transvection index. Then* $\operatorname{Inn} Q \cong G\langle N, \tau, m \rangle$ *and* $Q \cong Q\langle N, \tau, m \rangle$, *where N is a simple group, τ is an automorphism of finite order modulo* Inn N, *and $m \geqslant 1$. The quandle Q determines N up to isomorphism and m exactly. Also, $Q \cong Q\langle n, \tau_1, m \rangle \cong Q\langle n, \tau_2, m \rangle$ iff τ_1 is conjugate to τ_2 as elements of* Aut N.

Proof. Let $G = \operatorname{Inn} Q$ and $T = \operatorname{Trans} Q$. Let σ be conjugation by an element of G which is the symmetry of some element of Q. Lemmas 1 and 2 secure the hypotheses of Lemma 4 which in turn yields N, τ, and m. There is an isomorphism $G \to G\langle N, \tau, m \rangle$ which maps the element $x_0 \sigma(x_1) \cdots \sigma^{m-1}(x_{m-1})$ in Trans Q to $\langle x_0, x_1, \ldots, x_{m-1} \rangle$ in N^m and maps the element of G whose conjugation is σ to $\langle \mathbf{1}; 1 \rangle$ in $G\langle N, \tau, m \rangle$. In light of Lemma 4 all statements of this lemma except the last are evident. From the algebraic connectivity of Q, if there is a isomorphism $Q\langle n, \tau_1, m \rangle \cong Q\langle n, \tau_2, m \rangle$, then we may assume it maps $\langle \mathbf{1}; 1 \rangle$ to $\langle \mathbf{1}; 1 \rangle$. Furthermore, any such isomorphism extends to an isomorphism $G\langle n, \tau_1, m \rangle \cong G\langle n, \tau_2, m \rangle$, which, of course, determines an automorphism $\beta: N^m \cong N^m$. Hence, the two quandles are isomorphic iff there is an automorphism $\beta: N^m \to N^m$ such that $\beta \circ \sigma_1 = \sigma_2 \circ \beta$, where σ_i is determined by τ_i.

Case 1. Assume N is prime cyclic. In this case β, σ_1, and σ_2 may be interpreted as linear transformations of the vector space N^m. Hence, if $\beta \circ \sigma_1 = \sigma_2 \circ \beta$, then $\det \sigma_1 = \det \sigma_2$, which implies $\tau_1 = \tau_2$; equivalently, τ_1 is conjugate to τ_2.

Case 2. Assume N is nonabelian simple. Suppose there is an automorphism β of N^m such that $\beta \circ \sigma_1 = \sigma_2 \circ \beta$. An automorphism of N^m

must induce a permutation of the m factors of N^m. The automorphism σ_1 of N^m shifts the factors of N^m by one unit. Hence, by composing β with σ_1 some number of times, we may assume β leaves the first component of N^m invariant. It follows that β acts coordinatewise, moreover, that $\beta\langle x_0,\ldots, x_{m-1}\rangle = \langle\alpha(x_0),\ldots, \alpha(x_{m-1})\rangle$, where α is β restricted to any one coordinate. In terms of α, $\beta \circ \sigma_1 = \sigma_2 \circ \beta$ iff $\alpha \circ \tau_1 = \tau_2 \circ \alpha$. Thus, the quandles are isomorphic iff τ_1 is conjugate to τ_2 in Aut N. ∎

Now that we know Q determines τ only up to conjugation, given N a simple group, C a conjugacy class in Aut N, and $m \geqslant 1$, we may take $Q\langle N, C, m\rangle$ to be $Q\langle N, \tau, m\rangle$, where τ is any element in C, and weknow $Q\langle N, C, m\rangle$ is determined up to isomorphism if it is simple. Lemma 6 states when $Q\langle N, \tau, m\rangle$ is a simple quandle whose inner automorphism group is isomorphic to $G\langle N, \tau, m\rangle$. Theorem 7 summarizes the correspondence.

LEMMA 6. *Let N be a simple group, τ an automorphism of N of finite order modulo* Inn N, *and $m \geqslant 1$. Let $G = G\langle N, \tau, m\rangle$ and $Q = Q\langle N, \tau, m\rangle$. When N is prime cyclic, let its order be denoted p, and let a be such that $\tau(x) = ax$, $0 < a < p$. Then*

(i) *N^m is a minimal nontrivial normal subgroup of G iff either N is nonabelian, or N is prime cyclic and $X^m - a$ is an irreducible polynomial modulo p.*

Assume N^m is a minimal nontrivial normal subgroup of G. Then

(ii) $Z(G) = 1$.

(iii) $G' = N^m$.

(iv) *Q is nontrivial iff either $\tau \neq 1$ or $m \neq 1$.*

Assume also that Q is not trivial. Then

(v) *Q generates G.*

(vi) *Q is a simple quandle whose inner automorphism group is isomorphic to G.*

Proof. (i) *Case* 1. Assume N is a prime cyclic group. There is no proper nontrivial σ-invariant supgroup of N^m iff $\mathbb{Z}_p^m$ is an irreducible $\mathbb{Z}_p[\sigma]$-module where $\mathbb{Z}_p[\sigma] = \mathbb{Z}_p[X]/(X^m - a)$. Equivalently, $X^m - a$ is an irreducible polynomial modulo p.

Case 2. Assume N is nonabelian. Let M be a subgroup of N^m normal in G and containing a nontrivial element $\mathbf{x}$. Since M is closed under σ, we may assume the first coordinate x_0 of $\mathbf{x}$ is nontrivial. Since N is a nonabelian simple group, there is an element y_0 of N such that the commutator $[x_0, y_0]$

is nontrivial. Let $\mathbf{y} = \langle y_0, 1, \ldots, 1 \rangle$. Then $\mathbf{x}^{-1}(\mathbf{y}^{-1}\mathbf{x}\mathbf{y}) = \langle [x_0, y_0], 1, \ldots, 1 \rangle$ lies in M. Hence, $N \times 1 \times \cdots \times 1$ is contained in M, whence $N^m = M$.

(ii) With $T = N^m$, we may now apply Lemma 4 to derive $Z(G) = 1$.

(iii) This statement follows directly from the minimality of N^m and the construction of G.

(iv) Since $\langle \mathbf{1}; 1 \rangle$ is one element of Q, we need only find another. If $\tau \neq 1$, take $\langle y^{-1}\tau(y), 1, \ldots, 1; 1 \rangle$, where y is an element of N such that $\tau(y) \neq y$. If $\tau = 1$ and $m > 1$, take $\langle y, y^{-1}, 1, \ldots, 1; 1 \rangle$, where y is a nontrivial element of N.

(v) The quotient of two distinct elements of Q is a nontrivial element in N^m. Therefore, the intersection of N^m with the subgroup of G generated by Q is nontrivial; hence the intersection is N^m itself. Therefore, Q generates G.

(vi) Lemma 2 now implies statement (vi). ∎

For criteria for the irreducibility of $X^m - a$, see [6, p. 221].

THEOREM 7. *All and only simple quandles Q of order greater than two which have finite transvection index appear as $Q\langle N, C, m \rangle$ (described above and below Lemma 5), where N is a simple group, C is a conjugacy class in* Aut N *whose elements have finite order modulo* Inn N, *and $m \geqslant 1$, with the following exceptions*:

(1) *C is the conjugacy class of the identity while $m = 1$.*

(2) *N is prime cyclic of order p, τ in C is multiplication by a, $0 < a < p$, and the polynomial $X^m - a$ is reducible modulo p.*

For such a representation, Q determines N up to isomorphism and determines C and m exactly. The simple abelian quandles correspond to those triples $\langle N, C, m \rangle$, where N is prime cyclic. ∎

4. Simple Involutory Quandles

An *involutory quandle* is a 2-quandle, that is, a quandle satisfying the identity $(x \rhd y) \rhd y = x$. The symmetries of an involutory quandle are all involutions. Involutory quandles are called "keys" by Takasaki [11], "symmetric sets" by Nobusawa [9], and "symmetric spaces" by Doro [2]. See Loos [7] for an explanation of symmetric spaces in terms of the binary operation denoted here by $x \rhd y$. Nobusawa [10] and Nagao [8] discuss simple involutory quandles.

The core of a group G, Core G, as defined by Bruck [1] for the more general case of Moufang loops, is the underlying set of the group along with the operation $x \rhd y = yx^{-1}y$. This operation is not to be confused with conjugation; the core of one group, however, is likely to be a conjugacy class of involutions of some other group. Cores of groups are involutory quandles.

COROLLARY 8. *A simple involutory quandle is either isomorphic to* Core N, *where N is a simple group or isomorphic to a conjugacy class of involutions in a nonabelian simple group.*

Proof. By the above theorem every simple involutory quandle appears as $Q\langle N, \tau, m\rangle$, where $\sigma^2 = 1$; hence $m \leqslant 2$. When $m = 2$, we have $\tau = 1$, which gives $Q\langle N, \tau = 1, m = 2\rangle$, a quandle which is isomorphic to Core N. When $m = 1$, then $\tau \neq 1$ and $\tau^2 = 1$, which gives $Q\langle N, \tau, m = 1\rangle$, a conjugacy class of involutions in N. ∎

5. SIMPLE QUANDLES WITH INFINITE TRANSVECTION INDEX

It is easy to show there are no simple abelian quandles Q for which Inn Q/Trans Q is infinite. There are at least two types of nonabelian simple quandles with infinite transvection index.

(i) $Q\langle N$ nonabelian simple, $\tau = 1$, $m = \infty\rangle$.

(ii) $Q\langle N$ nonabelian simple, τ, $m < \infty\rangle$, where the order of τ modulo Inn N is infinity.

The constructions of these quandles and their associated groups is analogous to the finite case. The author expects there are other types without analogue in the finite case, perhaps some which are not closely related to simple groups.

REFERENCES

1. R. H. BRUCK, "A Survey of Binary Systems," Springer-Verlag, Berlin/New York, 1958.
2. S. DORO, Simple Moufang loops, *Math. Proc. Cambridge Philos. Soc.* **83** (1978), 377–392.
3. A. W. GOLDIE, The Jordan–Hölder theorem for general abstract algebras, *Proc. London Math. Soc. (2)* **52** (1950), 107–131.
4. G. GRÄTZER, "Universal Algebra," Van Nostrand, Princeton, N.J., 1968.
5. D. JOYCE, A classifying invariant of knots, the knot quandle, *J. Pure Appl. Algebra* **23** (1982), 37–66.
6. S. LANG, "Algebra," Addison–Wesley, Reading, Mass., 1969.
7. O. LOOS, "Symmetric Spaces," Benjamin, New York, 1969.

8. H. NAGAO, A remark on simple symmetric sets, *Osaka J. Math.* **16** (1979), 349–352.
9. N. NOBUSAWA, On symmetric structures of a finite set, *Osaka J. Math.* **11** (1974), 569–575.
10. NOBUSAWA, Simple symmetric sets and simple groups, *Osaka J. Math.* **14** (1977), 411–415.
11. M. TAKASAKI, Abstractions of symmetric functions, *Tôhoku Math. J.* **49** (1943), 143–207 (Japanese). *Math. Rev.* **9**, p. 8.